

In the present work we study algebraic attacks and cascading fast algebraic attack on stream ciphers using in their construction linear feedback shift registers. For deeper understanding of attacks we present some facts which are needed to know from theory of linear recurrence sequences in first chapter. We show their connection to formalized description of construction we attack. In second chapter we show algebraic attacks on both ciphers using memory or memoryless. We introduce definitions of annihilator and algebraic immunity of Boolean function and show their main properties. In third chapter we use knowledge from first two chapters and show process and principle of fast algebraic attack.